



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/920,740      | 08/03/2001  | Marco Martens        | YOR920000722US1     | 5936             |

30743 7590 07/18/2007  
WHITHAM, CURTIS & CHRISTOFFERSON & COOK, P.C.  
11491 SUNSET HILLS ROAD  
SUITE 340  
RESTON, VA 20190

|          |
|----------|
| EXAMINER |
|----------|

AGWUMEZIE, CHARLES C

|          |              |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

3621

|           |               |
|-----------|---------------|
| MAIL DATE | DELIVERY MODE |
|-----------|---------------|

07/18/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.



## **DETAILED ACTION**

### **Status of Claims**

1. Claims 2, 4, 14, 26, 31, and 33 are cancelled. Claims 1, 3, 5-13, 15-25, 27-30, 32, and 34-38, are amended. Claims 39-44 are newly added.

### ***Amendments to Specification***

2. The amendments to the Specification filed on April 23, 2007 relating to page 1, updating the status of the copending applications and on page 12, correcting the typographical errors is hereby acknowledged and entered.

### ***Response to Arguments***

3. Applicant's arguments with respect to claims 1-13, 25-30, and 33-35 have been considered but are moot in view of the new ground(s) of rejection. However Applicant argues that no check is remotely suggested by the combination of Davis et al and Buchanan et al.

In response, Examiner respectfully disagrees and asserts that a check is a document. Davis' document is covered or characterized by having critical fields encrypted with keys which is known by those that need to know and/or authorized to know it.

Applicant further argues that in order to further protect the check against fraud, the cryptographic function is indexed by a number corresponding to field k so that each

Art Unit: 3621

line comprises different encryptions of X such that each cryptographic function is a family of different cryptographic functions.

In response Davis et al discloses that the method of using multiple and/or different encryption algorithms (different family of encryptions) and/or keys, for different fields in a document that need different levels of security, thus providing selective data encryption technique as implemented by the Applicant (col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10).

Applicant further argues that Davis et al is used to protect document with different level of security such as various persons or group of persons are limited in level of access they are permitted to certain of the different elements of the document whereas applicant's invention is intended to prevent fraud by protecting the entire document i.e. the check.

In response, Davis is intended to protect the entire document as well as in a need to know basis. The levels of access/permissions in Davis et al is simply an added security. The general intended purpose is to protect the document from authorized access or fraud. Alternatively Buchanan is intended to protect the check from fraud.

Applicant further argues that Buchanan failed to cure the deficiencies of Davis because there is no suggestion in Buchanan et al of a check wherein critical fields are covered by a large number of lines of fine print comprising encrypted versions of a unique identifier...

In response, Examiner thanks Applicant for at least conceding that Buchanan discloses a check that is deposited from a remote location different from a bank.

Art Unit: 3621

However the combination of Davis et al encryption style and Buchanan's check does clearly disclose the claimed invention as shown in the rejections.

### ***Specification***

4. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 C.F.R. §1.75(d)(1), MPEP §608.01(o), and MPEP §2181. Correction of the following is required:

- a. The "means for printing checks"; "digitizing means for generating"; "extracting means for extracting" and "comparing means for comparing" as recited in claim 39.
- b. The "second extracting means for extracting" and "second comparing means for comparing" as recited in claim 40.
- c. The "third extracting means for extracting" and the "third comparing means for comparing" as recited in claim 41.

### ***Claim Rejections - 35 USC § 112***

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

**Claim 39, 40, and 41,** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claims are replete with errors. Some examples follow:

- a. In claim 39, it is unclear what is the corresponding structure (and the equivalents

thereof) of the "means for printing checks"; "digitizing means for generating"; "extracting means for extracting" and "comparing means for comparing"

b. In claim 40, it is unclear what is the corresponding structure (and the equivalents thereof) of the "second extracting means for extracting" and "second comparing means for comparing"

c. In claim 41, it is unclear what is the corresponding structure (and the equivalents thereof) of the "third extracting means for extracting" and the "third comparing means for comparing"

Regarding all the "means for" phrases, Applicants are also reminded, "For claim clauses containing functional limitations in 'means for' terms pursuant to § 112 ¶ 6, the claimed function and its supporting structure in the specification must be presented with sufficient particularity to satisfy the requirements of § 112 ¶ 2." *S3 Inc. v. nVIDIA Corp.*, 259 F.3d 1364, 1367, 59 USPQ2d 1745, 1747 (Fed. Cir. 2001) (citations omitted). In other words, "[f]ailure to describe adequately the necessary structure, material, or acts corresponding to a means-plus-function limitation in the written description means that the drafter has failed to comply with Section 112, Para. 2." *Atmel Corp. v. Information Storage Devices, Inc.*, 198 F.3d 1374, 1380 53 USPQ2d 1225, 1229 (Fed. Cir. 1999) citing *In re Dossel*, 115 F.3d 942, 945, 42 USPQ2d 1881, 1884 (Fed. Cir. 1997)).

### ***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 3621

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**Claims 1, 3, 5-13, 15-17, 18, 19-24, 25, 27-30, 32, 34-35, and 36-38**, are

rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al U.S. Patent No. 6,961,849 B1 in view of Buchanan et al U.S. Patent No. 7,181,430 B1.

As per **claims 1, 25 and 39**, Davis et al discloses a method of protecting a check which will be transformed into a value bearing instrument after adding additional markings to the check from fraudulent alteration of the markings comprising the steps of:

generating encryptions of a unique identifier X of the document, the unique identifier X being a check data including a bank ID, an account ID number, and a check number printed on the check the encryptions being  $\text{Sign}_{k,0}(X)$ , where  $\text{Sign}_{k,0}(X)$  is a cryptographic function or family thereof which is known only to an institution which issues the check,  $\text{Sign}_{k,o}(X)$  being used to authenticate the check (fig. 5; col. 18, lines 40-65; ...key strength identifier or encryption algorithm identifier or document identifier...); and

covering each critical field k,  $k=1,2,3, \dots$ , of the check where markings are to be added with a large number of lines of fine print, the lines of fine print comprising the cryptographic function Sign, the critical fields k including a date field, a payee field, amount fields, a payer's signature field, and an endorser's field (see fig. 4; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; ...using multiple and/or different encryption

algorithms and/or keys, for different fields in a document that need different levels of security...provide selective data encryption technique...).

What Davis does not explicitly teach is

the unique identifier X being a check data including a bank ID, an account ID number, and a check number printed on the check. Davis however discloses that the system is useful for data that is to be securely stored, such as the account records for customers of a bank or credit company.

Buchanan discloses that the document is a check (see figs. 1, 5, and 7; ...checks inherently contains a bank ID, an account ID number, and a check number...).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method of protecting a check document from fraudulent alteration, wherein the document is a check in order to specifically apply the method to check data thus ensuring security of remote deposit of checks.

As per claims 3, 27, and 34, Davis et al further discloses the method of protecting a check from fraudulent alteration, wherein each critical field k of the document, in addition to being covered by the encrypted version of X,  $\text{Sign.sub.k,0(X)}$ , is covered with another encrypted version of X,  $\text{Sign.sub.k(X)}$ , where  $\text{Sign.sub.k(X)}$  is another cryptographic function or family thereof different from the cryptographic function  $\text{Sign.sub.k,0(X)}$  which is known to a larger number of authorized institutions for performing an initial authentication of the check (col. 5, lines 10-30, 45-50; 60-65; col. 6,



Art Unit: 3621

lines 5-10; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security).

As per claims 5, 28, and 35, Davis et al further discloses the method of protecting a check from fraudulent alteration, wherein each critical field  $k$  of the check, in addition to being covered by encrypted versions of  $X$ ,  $\text{Sign.sub.k}(X)$  and  $\text{Sign.sub.k,0}(X)$ , is covered with a third encrypted version of  $X$ ,  $\text{Sec.sub.k}(X)$ , where  $\text{Sec.sub.k}(X)$  is another cryptographic function or family thereof different from the cryptographic functions  $\text{Sign.sub.k,0}(X)$  and  $\text{Sign.sub.k}(X)$  which is known to a small group within the institution which issues the check for performing final authentication of the check (see fig. 4; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; col. 16, line 60-col. 17, line 30; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security).

As per claims 6, 29 and 42, Davis et al further discloses the method of protecting a check from fraudulent alteration, further comprising the step of indexing the cryptographic functions  $\text{Sign.sub.k}$ ,  $\text{Sign.sub.k,0}$  and  $\text{Sec.sub.k}$ , by a number corresponding to the field  $k$ , so that each line comprises different encryptions of  $X$  such that each cryptographic function  $\text{Sign.sub.k}(X)$ ,  $\text{Sign.sub.k,0}(X)$  and  $\text{Sec.sub.k}(X)$  is a family of different cryptographic functions (see fig. 4; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; col. 16, line 60-col. 17, line 30; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different

Art Unit: 3621

levels of security).

As per **claims 7 and 30**, Davis et al further discloses the method of protecting a check from fraudulent alteration, wherein the families of cryptographic functions Sign.sub.k, Sign.sub.k,0 and Sec.sub.k prevent cryptographic functions which have been obscured at different places by marks added to the check from being used to reconstitute the full cryptographic function (see fig. 4; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; col. 16, line 60-col. 17, line 30; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security).

As per **claim 8**, Davis et al further discloses the method of protecting a check from fraudulent alteration, wherein electronic deposit of a check transformed into a value bearing instrument comprises the steps of:

scanning the check with a scanner to generate a digitized version of the check (see fig. 7c; col. 26, lines 25-45; col. 27, line 55-col. 28, line 10); and

transmitting the digitized version of the check for deposit (see fig. 7c; col. 1, lines 25-35; col. 26, lines 25-45).

As per **claim 9**, Davis et al further discloses the method of protecting a check from fraudulent alteration, wherein electronic deposit of a check transformed into a value bearing instrument further comprises the step of endorsing the document, if

needed, having printed thereon encryptions in at least selected locations where markings are added to transform the check into a value bearing instrument, the act of endorsing obscuring some of the encryptions (col. 1, lines 25-35; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; col. 16, line 60-col. 17, line 30; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security).

As per **claim 10**, Davis et al further discloses the method of protecting a check from fraudulent alteration, wherein electronic deposit of a check transformed into a value bearing instrument further comprises the steps of:

generating a digitized version of the check in at least selected locations where markings are added to transform the check into value bearing instrument(see fig. 7c; col. 26, lines 25-45; col. 27, line 55-col. 28, line 10; ..generating one or more encryption keys and encrypting selected elements of the document e.g. payroll information...);

extracting from the digitized version of the check the unique identifier X and a corresponding digital encryption of X,  $\text{Sign.sub.k}(X)$ , which is known to a large number of authorized institutions (col. 2, lines 10-40; col. 3, lines 25-35); and

comparing a decrypted version of  $\text{Sign.sub.k}(X)$  to the unique identifier X as an initial authentication of the check (col. 2, lines 50-65).

What Davis et al does not explicitly disclose is that the document is a check.

Buchanan discloses that the document is a check (see figs. 5 and 7).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method of generating a digitized version of the check in at least selected locations where markings are added to transform the check into value bearing instrument in view of the teachings of Buchanan et al in order to specifically apply the method to check data thus ensuring security of remote deposit of checks.

As per **claim 11**, Davis et al further discloses the method of protecting a check from fraudulent alteration, wherein electronic deposit of a document transformed into a value bearing instrument further comprises the steps of:

extracting from the digitized version of the check the unique identifier X and a corresponding digital encryption of X,  $\text{Sign.sub.k,0(X)}$ , which is known only to an institution that issues the check (col. 2, lines 10-40; col. 3, lines 25-35); and

comparing a decrypted version of  $\text{Sign.sub.k,0(X)}$  to the unique identifier X as a further authentication of the check (col. 2, lines 50-65).

As per **claim 12**, Davis et al further discloses the method of protecting a check from fraudulent alteration, wherein electronic deposit of a document transformed into a value bearing instrument further comprises the steps of:

extracting from the digitized version of the check the unique identifier X and a corresponding digital encryption of X,  $\text{Sec.sub.k(X)}$ , which is known to a small group within the institution that issues the check (col. 2, lines 10-40; col. 3, lines 25-35); and

comparing a decrypted version of  $\text{Sec.sub.k}(X)$  to the unique identifier  $X$  as a final authentication of the check (col. 2, lines 50-65).

As per **claim 13**, Davis et al further discloses the method of protecting a check from fraudulent alteration, wherein portions of the lines of fine print are obscured by writing added to the check when transforming the document into a value bearing instrument (col. 1, lines 25-35).

As per **claim 15**, Davis et al further discloses the method of protecting a check from fraudulent alteration, wherein an issuing bank chooses a first secret key  $\text{Sign.sub.k}$  using a secure cryptographic generator (SCG), further comprising the steps of:

computing the first family of encrypted functions  $\text{Sign.sub.k}(X)$  (see fig. 4; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; col. 16, line 60-col. 17, line 30; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security); and

communicating the key  $\text{Sign.sub.k}$  to banks and other authorized institutions involved in depositing of checks, the family of encrypted functions  $\text{Sign.sub.k}(X)$  allowing the payee's bank to perform a first authentication of the check (see fig. 7c; col. 1, lines 25-35; col. 26, lines 25-45).

What Davis does not explicitly teach is that the document is check and process involved in depositing of checks.

Buchanan et al discloses that the document is check and the process involved in depositing the check (see figs. 5 and 7)

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method of protecting a document from fraudulent alteration, wherein the document is a check and the process involved in depositing the check in view of the teachings of Buchanan et al in order to specifically apply the method to check data thus ensuring security of remote deposit of checks.

As per claim 16, Davis et al discloses the method of protecting a check from fraudulent alteration, wherein an issuing bank chooses a second secret key Sign.sub.k,0 using a SCG, further comprising the steps of:

computing a second family of encrypted functions Sign.sub.k,0(X), key Sign.sub.k,0 remaining the exclusive property of the issuing bank (see fig. 4; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; col. 16, line 60-col. 17, line 30; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security); and

using SCGs, communicating the key Sign.sub.k,0 to all branches of the issuing bank where check clearing is done, the family of encrypted functions Sign.sub.k,0(X) being used exclusively by the issuing bank and branches involved in the clearing of checks (see fig. 4; col. 1, lines 25-35; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10;

col. 16, line 60-col. 17, line 30; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security).

As per claim 17, Davis et al further discloses the method of protecting a check from fraudulent alteration, wherein an issuing bank chooses a third secret key Sec.sub.k which is exclusively known to a small group within the issuing bank, further comprising the step of computing a third family of encrypted functions Sec.sub.k(X), the secret key Sec.sub.k being used by the issuing bank as final instrument to verify the check (see fig. 4; col. 1, lines 25-35; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; col. 16, line 60-col. 17, line 30; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security).

As per claim 18, Davis et al failed to explicitly disclose the method of protecting a check from fraudulent alteration, wherein the check is deposited by a payee electronically from a location remote from a bank or Automatic Teller Machine (ATM).

Buchanan et al discloses the method of protecting a document from fraudulent alteration, wherein the check is deposited by a payee electronically from a location remote from a bank or Automatic Teller Machine (ATM) (col. 1, lines 35-45; col. 2, lines 10-35).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method of protecting a check from fraudulent alteration, wherein the check is deposited

by a payee electronically from a location remote from a bank or Automatic Teller Machine (ATM) in view of the teachings of Buchanan et al in order to encourage the convenience of depositing check data from remote locations distinct from bank or ATM.

As per **claim 19**, Davis et al failed to explicitly disclose the method of protecting a check from fraudulent alteration, wherein electronic deposit of the check by a payee comprises the steps of:

endorsing the check having printed thereon encryptions in at least selected locations where information is written by a payer, the act of endorsing by the payee obscuring some of the encryptions; scanning the endorsed check with a scanner to generate a digitized version of the check; transmitting the digitized version of the check for deposit to the payee's bank. Davis however discloses that the system is useful for data that is to be securely stored, such as the account records for customers of a bank or credit company.

Buchanan et al discloses endorsing the check having printed thereon encryptions in at least selected locations where information is written by a payer, the act of endorsing by the payee obscuring some of the encryptions (see figs. 5 and 7; col. 2, lines 10-50);

scanning the endorsed check with a scanner to generate a digitized version of the check (see figs. 5 and 7); transmitting the digitized version of the check for deposit to the payee's bank (see figs. 5 and 7).



Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method of protecting a check from fraudulent alteration, wherein endorsing the check having printed thereon encryptions in at least selected locations where information is written by a payer, the act of endorsing by the payee obscuring some of the encryptions; scanning the endorsed check with a scanner to generate a digitized version of the check; transmitting the digitized version of the check for deposit to the payee's bank in view of the teachings of Buchanan et al in order to specifically apply the method to check data thus ensuring security of remote deposit of checks.

As per **claim 20 and 40**, Davis et al further discloses the method of protecting a check from fraudulent alteration, wherein electronic deposit of the check by a payee comprises the steps of:

extracting by the payee's bank from the digitized version of the check the unique identifier  $X$  and a corresponding digital encryption of  $X$ ,  $\text{Sign.sub.k}(X)$ , which is known to a large number of authorized institutions including the payee's bank (col. 2, lines 10-40; col. 3, lines 25-35); and

comparing by the payee's bank a decrypted version of  $\text{Sign.sub.k}(X)$  to the unique identifier  $X$  as an initial authentication of the check (col. 2, lines 50-65).

What Davis does not explicitly teach is that the document is a check. Davis however discloses that the system is useful for data that is to be securely stored, such as the account records for customers of a bank or credit company.

Buchanan discloses that the document is a check (see figs. 1, 5, and 7).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method of protecting a check from fraudulent alteration, wherein the document is a check in order to specifically apply the method to check data thus ensuring security of remote deposit of checks.

As per **claim 21 and 41**, Davis et al further discloses the method of protecting a check from fraudulent alteration, wherein electronic deposit of the check further comprises the steps of:

extracting from the digitized version of the check the unique identifier X and a corresponding digital encryption of X, Sign.sub.k,0(X), which is known only to a bank that issues the check (col. 2, lines 10-40; col. 3, lines 25-35); and

comparing by the payor's bank a decrypted version of Sign.sub.k,0(X) to the unique identifier X as a further authentication of the check (col. 2, lines 50-65).

What Davis does not explicitly teach is that the document is a check. Davis however discloses that the system is useful for data that is to be securely stored, such as the account records for customers of a bank or credit company.

Buchanan discloses that the document is a check (see figs. 1, 5, and 7).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method of protecting a check from fraudulent alteration, wherein the document is a

Art Unit: 3621

check in order to specifically apply the method to check data thus ensuring security of remote deposit of checks.

As per **claim 22**, Davis et al further discloses the method of protecting a check from fraudulent alteration, wherein electronic deposit of the check further comprises the steps of:

extracting from the digitized version of the check the unique identifier X and a corresponding digital encryption of X,  $\text{Sec.sub.k}(X)$ , which is known to a small group within the bank that issues the check (col. 2, lines 10-40; col. 3, lines 25-35); and

comparing a decrypted version of  $\text{Sec.sub.k}(X)$  to the unique identifier X as a final authentication of the check (col. 2, lines 50-65).

What Davis does not explicitly teach is that the document is a check. Davis however discloses that the system is useful for data that is to be securely stored, such as the account records for customers of a bank or credit company.

Buchanan discloses that the document is a check (see figs. 1, 5, and 7).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method of protecting a check from fraudulent alteration, wherein the document is a check in order to specifically apply the method to check data thus ensuring security of remote deposit of checks.

As per **claims 23 and 44**, Davis et al failed to explicitly disclose the method of

Art Unit: 3621

protecting a check from fraudulent alteration, further comprising the step of accessing a database by the payee's bank where the unique identifier X and first encrypted function Sign.sub.k(X) is registered to determine whether the check has been previously presented for deposit.

Buchanan et al discloses the method of protecting a check from fraudulent alteration, further comprising the step of accessing a database by the payee's bank where the unique identifier X and first encrypted function Sign.sub.k(X) is registered to determine whether the check has been previously presented for deposit (col. 13, line 45-col. 14, line 5; col. 17, lines 10-55; ...determines whether item is payable or not...).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method of protecting a check from fraudulent alteration, further comprising the step of accessing a database by the payee's bank where the unique identifier X and first encrypted function Sign.sub.k(X) is registered to determine whether the check has been previously presented for deposit in order to prevent fraud of deposit one same check multiple times.

As per **claim 24**, Davis et al failed to explicitly disclose the method of protecting a check from fraudulent alteration, further comprising the step of registering a check to be deposited by the payee with an SCG to prevent multiple deposits.

Buchanan et al discloses the method of protecting a check/document from fraudulent alteration, further comprising the step of registering a check to be deposited

by the payee with an SCG to prevent multiple deposits (col. 13, line 45-col. 14, line 5; col. 17, lines 10-55; ...determines whether item is payable or not...).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method method of protecting a check from fraudulent alteration, further comprising the step of registering a check to be deposited by the payee with an SCG to prevent multiple deposits in order to avoid multiple deposit one same check through the remote deposit of checks.

As per claim 32, Davis et al further discloses the check, wherein the act of adding markings to the check to transform the document into a value bearing instrument obscures some of the encryptions (fig. 4)

As per claim 36, Davis et al failed to explicitly disclose the check, wherein the encrypted function  $\text{Sign.sub.k(X)}$  are communicated to banks and other authorized institutions involved in depositing checks and the encrypted function  $\text{Sign.sub.k(X)}$  allows the payee's bank to perform a first authentication of the check. Davis however discloses that the system is useful for data that is to be securely stored, such as the account records for customers of a bank or credit company.

Buchanan et al discloses the check, wherein the encrypted function  $\text{Sign.sub.k(X)}$  are communicated to banks and other authorized institutions involved in depositing checks and the encrypted function  $\text{Sign.sub.k(X)}$  allows the payee's bank to

Art Unit: 3621

perform a first authentication of the check (see figs. 5 and 7; col. 9, line 40-col. 10, line 5).

Accordingly, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Davis et al and incorporate the method wherein the encrypted function  $\text{Sign.sub.k}(X)$  are communicated to banks and other authorized institutions involved in depositing checks and the encrypted function  $\text{Sign.sub.k}(X)$  allows the payee's bank to perform a first authentication of the check in view of the teachings of Buchanan et al in order to prevent fraud and ensure adequate security of remote deposit of checks.

As per **claim 37**, Davis et al further discloses the check, wherein key  $\text{Sign.sub.k,0}$  remains the exclusive property of the issuing bank and the encrypted function  $\text{Sign.sub.k,0}(X)$  is used exclusively by the issuing bank and branches involved in the clearing of checks (col. 3, lines 25-35; col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security).

As per **claim 38**, Davis et al further discloses the check, wherein secret key  $\text{Sec.sub.k}$  is exclusively known to the issuing bank and the encrypted function  $\text{Sec.sub.k}(X)$  is used by the issuing bank as a final instrument to verify the check (col. 3, lines 25-35).

As per claim 43, Davis et al further discloses the apparatus further comprising one or more secure cryptographic generators (SCGs) for computing the first family of encrypted functions  $\text{Sign}_k(X)$ , the second family of encrypted functions  $\text{Sign}_{k,0}(X)$ , and the third family of encrypted functions  $\text{Seck}(X)$  (col. 5, lines 10-30, 45-50; 60-65; col. 6, lines 5-10; ...using multiple and/or different encryption algorithms and/or keys, for different fields in a document that need different levels of security).

### ***Conclusion***

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

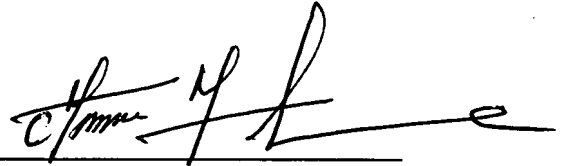
**Examiner's Note:** Examiner has cited particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that the applicant, in preparing the responses, fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **Charles C.L. Agwumezie** whose number is **(571) 272-6838**. The examiner can normally be reached on Monday – Friday 8:00 am – 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Andrew Fischer** can be reached on **(571) 272 – 6779**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.





Charlie Lion Agwumezie  
Patent Examiner  
Art Unit 3621

Acc  
June 26, 2007



ANDREW J. FISCHER  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 3600